CLAIMS:

1. A method of accessing an encrypted track on a removable media with a device, the track comprising frames having content, the method comprising:

authorizing the media;

decrypting the track by a process comprising:

(a) calculating a media unique key; and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed.

2. The method of claim 1, wherein authorizing the media comprises:

calculating a media key; and thereafter

calculating a media unique key from the media key; and thereafter

deleting the media key; and thereafter

calculating a session key from the media unique key; and thereafter

deleting the media unique key.

3. The method of claim 1, further comprising:

decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key; and

copying the singly encrypted title key from the media into a memory of the device.

4. The method of claim 2, wherein calculating the media key comprises:

(a) reading a first record of a media key block from a buffer;

(b) updating the buffer offset based on the length and type of the first record;

(c) reading another record of the media key block at the updated buffer offset; and

(d) repeating (a) - (c) until all necessary records of the media key block are read and the media key is calculated.

5. The method of claim 1, wherein the group of frames comprises less than one to about five seconds of content in a decoded or decompressed form.

6. The method of claim 1, wherein decrypting the track comprises decrypting one or more files, the files comprising the frames.

7. The method of claim 1, further comprising decoding and decompressing the track.

8. A method of accessing an encrypted data file on a removable media with a device, the data file comprising frames having content, the method comprising:

authorizing the media for a user session by a process comprising:

calculating a media key; and thereafter

calculating a media unique key from the media key; and thereafter

deleting the media key; and thereafter

calculating a session key from the media unique key; and thereafter

deleting the media unique key.

decrypting a doubly encrypted title key stored in the media with the session key to produce a singly encrypted title key;

copying the singly encrypted title key from the media into a memory of the device; and

decrypting the file by a process comprising:

(a) calculating the media unique key; and thereafter

(b) decrypting the title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key;

(f) repeating (a) through (e) until the entire file is completed.

9. The method of claim 8, wherein calculating the media key comprises:

dividing a media key block into chunks, the chunks comprising bytes of encrypted data; and

encrypting a key within the media key block by setting the buffer to read at an offset within a specific chunk of the block.

10. The method of claim 9, wherein decrypting the key comprises:

(a) calculating a media key from first record; and

(b) updating the buffer offset; and

(c) reading a second record at the updated buffer offset; and

(d) verifying the media key with a second record by comparing the calculated media key with a reference media key.

11. The method of claim 10, wherein the buffer offset is determined by the type and length of the first record of the media key block.

12. The method of claim 8, wherein the group of frames comprises less than one second to about five seconds of decompressed and decoded audio content.

13. A system for enabling a device to read an encrypted file having encrypted content from a media, and to write an encrypted file having encrypted content to a media, the system comprising:

a computing unit, and a system memory;

interface means for receiving commands from the device;

secure dynamic decryption means configured to:

(a) copy an encrypted title key from the media to a memory of the device,

(b) decrypt the encrypted title key,

(c) decrypt a portion of encrypted content with the decrypted title key,

(d) delete the decrypted title key, and

(e) repeat a-d such until all of the content of the file has been decrypted, and wherein the decrypted title keys reside in and are accessible only to the secure means of the system.

14. The system of claim 13, wherein the title key is in a decrypted state for the time it takes to decrypt 5 seconds or less of content in a decompressed and decoded state when played back.

15. The system of claim 13, further comprising a digital signal processor.

16. The system of claim 13, wherein the interface means and secure dynamic decryption means are stored in a system memory of the device.

17. The system of claim 16, wherein the interface means and secure dynamic decryption means are executed by the computing unit.

18. The system of claim 15, wherein the secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor.

19. The system of claim 18, wherein the interface means is executed by the digital signal processor.

20. A system that enables a device to decrypt a file having encrypted content on a secure medium, the system comprising:

one or more user interface modules for receiving commands from the device;

an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium;

a security engine for decrypting the encrypted content and the one or more encrypted keys sent from the secure medium to a memory of the device, the decrypted keys used to decrypt the encrypted content, wherein

the one or more keys are contained in an encrypted data segment, and

the security engine (a) decrypts one or more of the keys, (b) decrypts a portion of the encrypted content using the one or more decrypted keys, and (c) deletes the one or more decrypted keys, and (d) repeats (a) - (c) until all portions of the content are decrypted.

21. The system of claim 20, wherein the content is encoded in the AAC, MP3 or WMA format.

22. The system of claim 21, wherein the one or more keys are in a decrypted state for the time it takes to decrypt and process less than one second to about five seconds of decoded content.

23. The system of claim 20, wherein the data segment comprising the one or more encrypted keys is buffered and decrypted in fractional portions.

24. The system of claim 23, wherein the fractional portion is about 512 bytes.

25. The system of claim 20, wherein the device comprises a computing unit, system memory, and a hardware interface.

26. The system of claim 20, wherein the device further comprises a digital signal processor.

27. The system of claim 25, wherein the system is stored in the system memory of the device.

28. The system of claim 27, wherein the software system stored in the system memory is executed by the computing unit.

29. The system of claim 26, wherein the system is stored in RAM of the digital signal processor.

30. The system of claim 26, wherein a portion of the system is stored in the system memory of the device and a portion of the system is stored in RAM of the digital signal processor.

31. The system of claim 30, wherein the portion of the system stored in the RAM of the digital signal processor is executed by the digital signal processor.

32. The system of claim 30, wherein the portion of the system stored in the RAM of the digital signal processor comprises the security engine.

33. The system of claim 20, further comprising one or more engines for processing and transmitting audio, video or images, each engine comprising a secure application programming interface, the secure interface(s) for accessing the encrypted content and keys of the medium, and the non-secure interface(s) for accessing the unencrypted content of the medium.

34. The system of claim 33, further comprising a security manager module.

35. The system of claim 34, wherein the secure interface(s) communicate with the security manager module and module communicates with the security engine.

36. The system of claim 33, further comprising a device driver, the security engine accessing the content and keys through the device driver.

37. The system of claim 33, wherein each of the one or more engines for processing and transmitting audio, video or images further comprising a non-secure application programming for accessing unencrypted content of the medium.

38. The system of claim 20, wherein the security engine further comprises a random number generator, the generator utilizing two or more system timers to create the random number.

39. The system of claim 38, wherein the generator increases the natural frequency update of the timer ticks used to create the random number.